Practical Challenges in Defense Against Modern Ransomware

Dr. Pranshu Bajpai

July 14th, 2021

NCCoE, NIST Workshop on Preventing and Recovering from Ransomware and Other Destructive Cyber Events

MOTOROLA SOLUTIONS

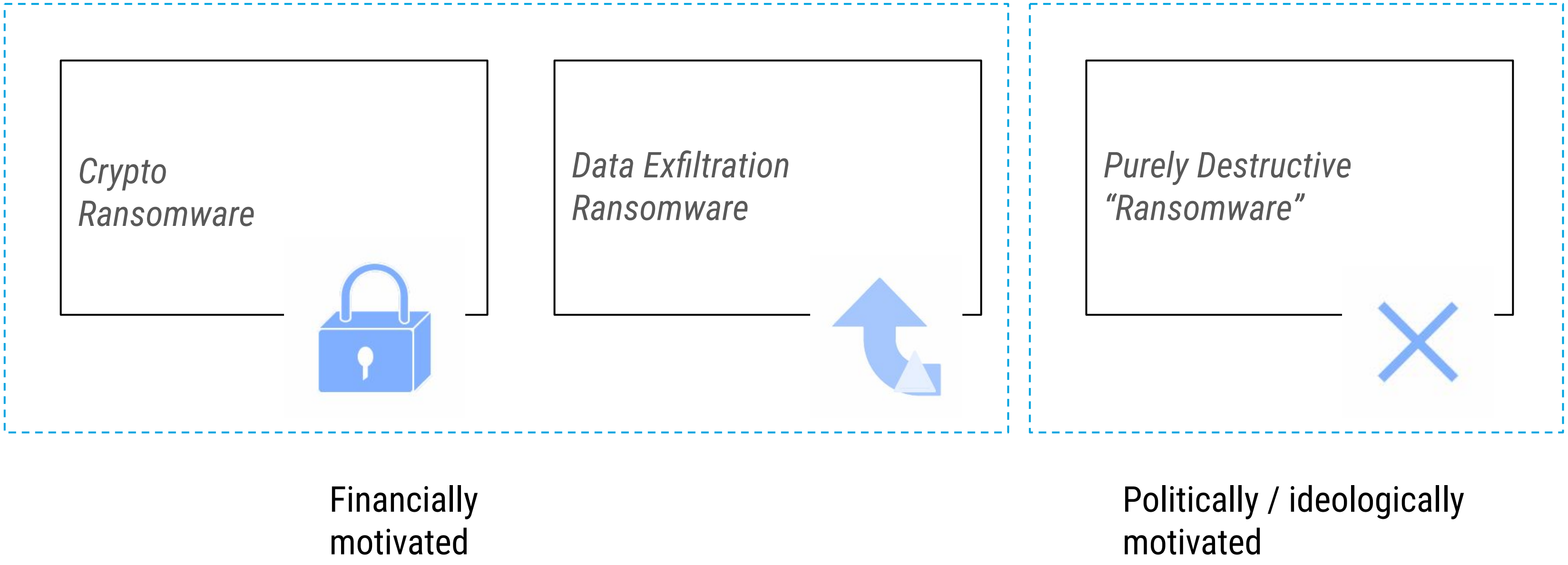
Agenda

- Ransomware Threat Comprehension
- Ransomware Response Playbooks
- Industry-wide Collaborative Efforts

RANSOMWARE THREAT COMPREHENSION

Redefining Ransomware

A type of malware that attempts financial extortion by gaining leverage over the victim's computing resources



Crypto Ransomware

Data Exfiltration Ransomware

Purely Destructive "Ransomware"

Financially motivated

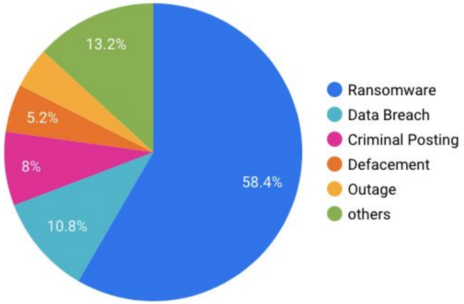
Politically / ideologically motivated

Overall Threat Landscape - *Public Sector*

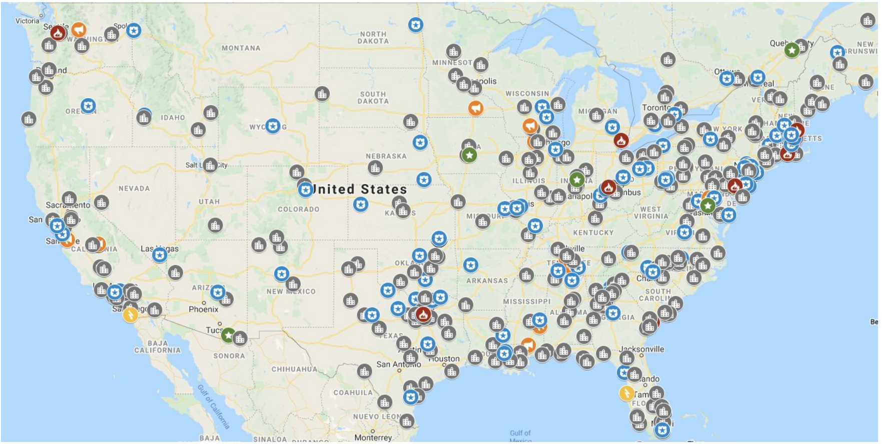
- Public sectors systems under increased threat
- *Diversity* and *refinement* in attack vectors
- General *responsiveness* of ransomware actors
- *Targeted* and *manual* ransomware attacks gaining traction
- Increasing ransom demands indicate successful business model

Example scenario

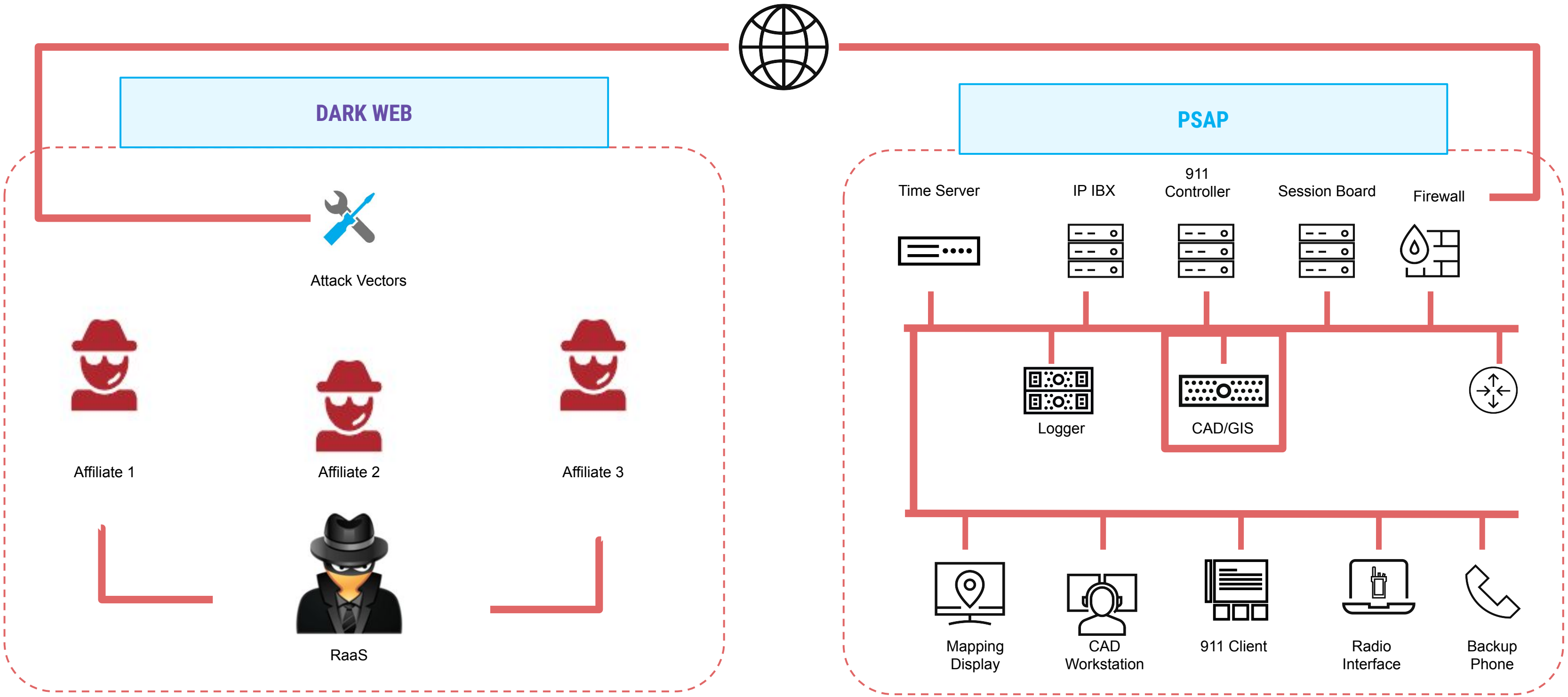
- Organization hit with a ransomware
    - Attack vector: Compromised credentials
    - Impact: Multiple systems
    - Demand: $100,000 - $(MILLIONS)



- Municipality
- Police Department
- Federal Govt. or Military
- Dispatch Center
- Fire Department
- SCADA or Utility
- Prison
- EMS Service



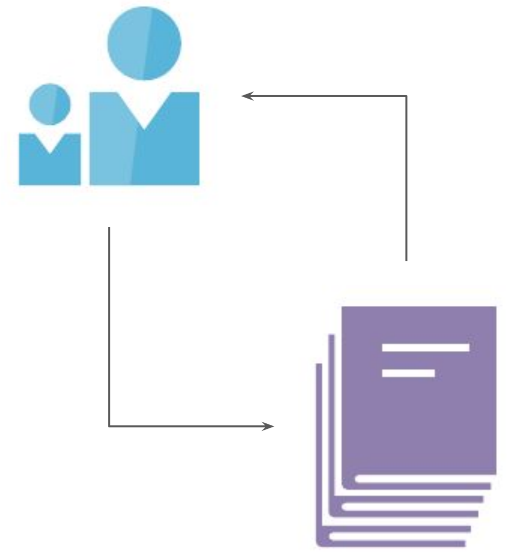
Ransomware-as-a-Service (RaaS) *versus* The Victim



RANSOMWARE RESPONSE PLAYBOOKS

Ransomware Incident Response (FAQs)

- When does ransomware response begin?
  - Planning versus execution
- How regularly should the response playbook be updated?
  - Establishing update cadence
- How should the playbook be communicated?
  - Ensuring communication and comprehension
- When should response be escalated?
  - Establishing escalation criteria
- How to resolve ambiguity in the response playbooks?
  - Defining terms, teams, stakeholders, system tiers
- How to ensure proper containment?
  - Establishing timely containment procedures
- How to maintain an updated list of internal and external resources?
  - Enumerating response resources



Effective Ransomware Response Playbooks

1. **KNOW YOUR ENVIRONMENTS** - *Hardware, Software, Applications, Data Flows*
2. **KNOW YOUR ADVERSARY** - *Who is attacking and how might they do it?*
3. **OUTLINE TEAMS AND RESPONSIBILITIES** - *Who is accountable / responsible for what?*
4. **OUTLINE INTERNAL AND EXTERNAL STAKEHOLDERS** - *Who should be involved?*
5. **UNDERSTAND, TEST, IMPROVE, REPEAT** - *Well-understood, Well-practiced response activities*
6. **ORDER OF OPERATIONS** - *Priorities and timelines*

Challenges

Strategic

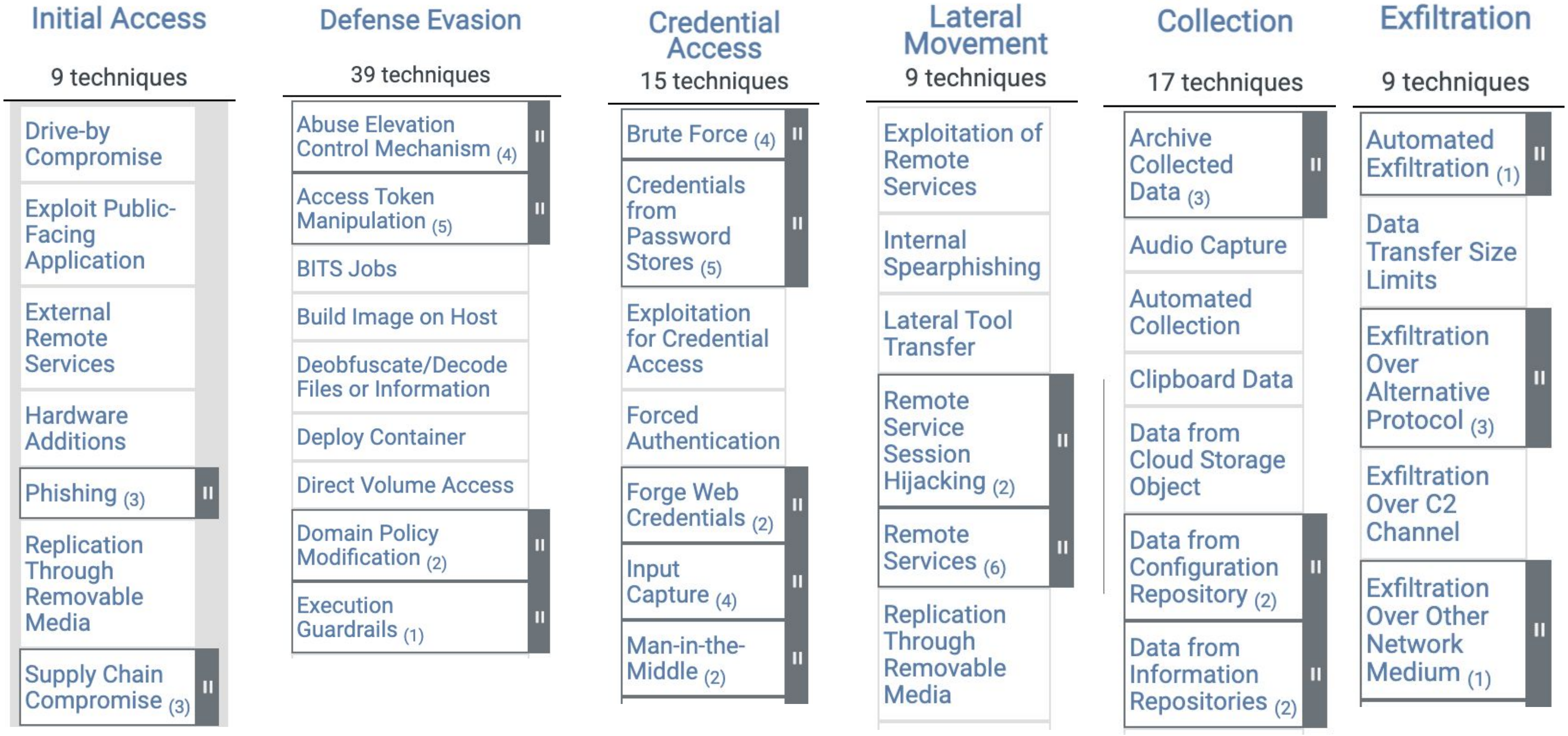
- Creating a consistent criteria for assessing the true impact, scope, severity
- Tapping into the relevant threat intelligence feeds to update response strategy
- Comprehending the true cost of a ransomware incident

Tactical

- Determining the appropriate internal and external stakeholders to be involved
- Assigning responsibilities while minimizing gaps and overlaps in response efforts
- Working with the affected teams to understand the architecture and technology stack

INDUSTRY-WIDE COLLABORATION

Standardized Threat Mapping (MITRE ATT&CK)



Initial Access	Defense Evasion	Credential Access	Lateral Movement	Collection	Exfiltration
9 techniques	39 techniques	15 techniques	9 techniques	17 techniques	9 techniques
Drive-by Compromise	Abuse Elevation Control Mechanism (4)	Brute Force (4)	Exploitation of Remote Services	Archive Collected Data (3)	Automated Exfiltration (1)
Exploit Public-Facing Application	Access Token Manipulation (5)	Credentials from Password Stores (5)	Internal Spearphishing	Audio Capture	Data Transfer Size Limits
External Remote Services	BITS Jobs	Exploitation for Credential Access	Lateral Tool Transfer	Automated Collection	Exfiltration Over Alternative Protocol (3)
Hardware Additions	Build Image on Host	Forced Authentication	Remote Service Session Hijacking (2)	Clipboard Data	Exfiltration Over C2 Channel
Phishing (3)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Remote Services (6)	Data from Cloud Storage Object	Exfiltration Over Other Network Medium (1)
Replication Through Removable Media	Deploy Container	Input Capture (4)	Replication Through Removable Media	Data from Configuration Repository (2)	
Supply Chain Compromise (3)	Direct Volume Access	Man-in-the-Middle (2)		Data from Information Repositories (2)	
	Domain Policy Modification (2)				
	Execution Guardrails (1)				

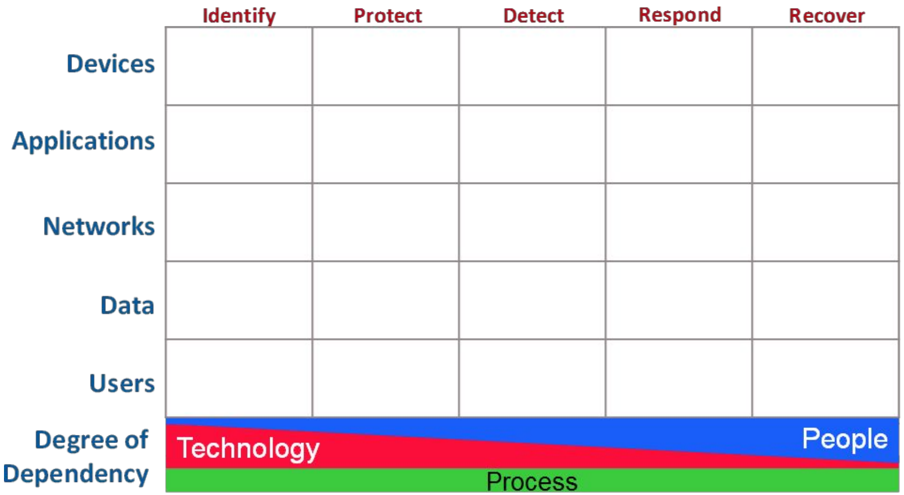
Rapid Standardized Communication

Pre-incident analysis

- Identify your specific security technology stack
- Identify *gaps* in security coverage
- Address gaps and reassess periodically

Post-incident assessment

- Identify gaps that led to the ransomware incident
- Identify additional security controls required to address these gaps
- Share lessons learned with the community



	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					

Degree of Dependency
Technology
People
Process

https://cyberdefensematrix.com/

Conclusion

- Post-breach assumption: strategize next steps
  - Zero-trust architectures
  - Response strategies
  - Business continuity and disaster recovery (beyond just backups)
- Know thy enemy:
  - RaaS, tactics, techniques, and procedures (TTPs), motives
  - Develop internal and/or external threat intelligence channels
- Know thyself:
  - Technology stacks, mission-critical environments
  - Gaps in security controls, visibility, detection methodologies
- Industry-wide collaboration:
  - Timely information-sharing via trusted partners

THANK YOU

MOTOROLA SOLUTIONS